Arctic User's Manual

Arctic GPRS Router (2270)

Firmware Version 5.0.7
Document Version 1.6
April 2010

Copyright and Trademark

Copyright © 2008-2010, Viola Systems Ltd. All rights to this manual are owned solely by Viola Systems Ltd. (referred elsewhere in this User's Manual as Viola Systems). All rights reserved. No part of this manual may be transmitted or reproduced in any form or by any means without a prior written permission from Viola Systems.

Ethernet™ is a trademark of XEROX Corporation. Windows™ and Internet Explorer™ are trademarks of Microsoft Corporation. Netscape™ is a trademark of Netscape Communications Corporation. All other product names mentioned in this manual are the property of their respective owners, whose rights regarding the trademarks are acknowledged.

Viola Systems Ltd.

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

E-mail: info@violasystems.com

Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: http://www.violasystems.com

Disclaimer

Viola Systems reserves the right to change the technical specifications or functions of its products or to discontinue the manufacture of any of its products or to discontinue the support of any of its products without any written announcement and urges its customers to ensure that the information at their disposal is valid.

Viola software and programs are delivered “as is”. The manufacturer does not grant any kind of warranty including guarantees on suitability and applicability to a certain application. Under no circumstance is the manufacturer or the developer of a program responsible for any damage possibly caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are the sole property of Viola Systems. Any transfer, licensing to a third party, leasing, renting, transportation, copying, editing, translating, modifying into another programming language or reverse engineering for any intent is forbidden without the written consent of Viola Systems.

Viola Systems has attempted to verify that the information in this manual is correct with regard to the state of products and software on the publication date of the manual. We assume no responsibility for possible errors which may appear in this manual. Information in this manual may change without prior notice from Viola Systems.

Declaration of Conformity

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name: Viola Systems Ltd.

Manufacturer's Address:

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

declares that this product:

Product Name:

Arctic GPRS Router

conforms to the following standards:

EMC:

EN 55022 Emission Test (Class A)

1. Radiated Emissions (30-1000MHz)
2. Conducted Emissions (0.15-30MHz)

EN 50082-1 Immunity Test

1. IEC 801-3: Radio Frequency Electromagnetic Field
2. IEC 801-2: Electrostatic Discharge
3. IEC 801-4: Fast Transients, AC Power Ports and Signal cables

Supplementary Information:

"The product complies with the requirements of the Low Voltage Directive 73/23/EEC and EMC directive 89/336/EEC."

Warning!
This is a Class A product. In a domestic environment this product may cause radio Interference which may make it necessary for the user to take adequate measures.

Manufacturer's Contact Information:

Viola Systems Ltd.

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

Phone: +358 20 1226 226

Fax: +358 20 1226 220

Warranty and Safety Instructions

Read these safety instructions carefully before using the products mentioned in this manual:

Warranty will be void if the product is used in any way in contradiction with the instructions given in this manual or if the product has been tampered with.

The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.

To prevent damage both the product and any terminal devices must always be switched OFF before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. Before connecting any power cables the output voltage of the power supply should be checked.

This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment or as part of such equipment in any hazardous environment requiring fail- safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of Viola Systems manufactured hardware or software could lead directly to death, personal injury, or severe physical or environmental damage.

Revisions

Date	Document Version	Firmware Version	Description of changes
01/2004	1.0		Manual released
06/2004	1.1		Minor modifications and HW update
10/2005	1.4		General text related corrections / Chapter 5 - Firewall rewritten
06/2008	1.5	5.0.7	Firmware 5.0.7 updated
04/2010	1.6		Lay-out changed. Side Panel description updated.

Contents

COPYRIGHT AND TRADEMARK 2
DISCLAIMER 3
DECLARATION OF CONFORMITY 4
WARRANTY AND SAFETY INSTRUCTIONS 5
REVISIONS 6
1. INTRODUCTION 9
1.1 About this User's Manual 9
1.2 The Arctic Platform 9
2. PHYSICAL INTERFACES 11
2.1 Front Panel Description 11
2.2 Back Panel Description 13
2.3 Side Panel Description 14
2.4 Product Information Label 15
2.5 Firmware Version 16
3. GETTING STARTED 17
3.1 Unpacking the Arctic 17
3.2 Installation of the Arctic 17
3.3 Setting of the IP Address Using an HTML Browser 17
3.4 Setting of the IP Address Using a Console 19
4. ARCTIC CONFIGURATOR TOOL 22
4.1 Login to Arctic Configurator 22
4.2 General Usage of the Arctic Configurator 23
5. ARCTIC SOFTWARE CONFIGURATION 24
5.1 System Menu 24
5.2 Network Menu 24
5.2.1 Ethernet 25
5.2.2 GPRS 26
5.2.3 Dial-in 27
5.2.4 SSH-VPN 28
5.2.5 L2TP-VPN 29
5.2.6 GRE 31
5.2.7 Monitor 31
5.2.8 Routing 32
5.2.9 S-NAT 33
5.2.10 D-NAT 33
5.2.11 DNS Update 34
5.2.12 DynDNS Client 34
5.2.13 NTP Client 35
5.2.14 SMS Config 35
5.3 Firewall Menu 36
5.4 Service Menu 38
5.4.1 WWW 38
5.4.2 Telnet 38

5.4.3 DHCP Server 38
5.5 Tools Menu 39
6. GPRS 41
6.1 Placing Arctic 41
6.2 GPRS Antenna 41
6.3 SIM Card and Card Holder 42
6.4 Configuring Arctic's GPRS Settings 42
6.5 Useful GSM/GPRS Information 43
7. TROUBLESHOOTING 45
7.1 Common Problems 45
SPECIFICATIONS 46
LIMITED WARRANTY 47
TECHNICAL SUPPORT 48

1 Introduction

Viola Arctic product family offers industrial quality connectivity devices for custom-built wireless and wired device management solutions.

1.1 About this User's Manual

This User's Manual describes the operation of the Arctic GPRS Router. All devices in this User's Manual are referred to as Arctic, unless otherwise mentioned. This manual provides introductory information as well as detailed instructions on how to set up and manage the Arctic as part of a network environment. It is intended for anyone involved in installing and managing Arctic devices. It is assumed that the reader of this manual is familiar with basic working principles of Internet technology.

Figure 1. *Arctic GPRS Router*

1.2 The Arctic Platform

The Arctic platform utilizes a number of wireless or fixed line interfaces depending on your specific requirements. Arctic is a customizable technology allowing users to develop solutions for their own applications. Arctic devices have been designed to withstand the requirements of extreme environments and industrial use.

Technical Features Summary

The following are the functional components in the Arctic GPRS Router device.

Details of the each components are listed below:

HARDWARE

CPU Platform:

- 32-bit RISC microcontroller
- 32 MB RAM
- 8 MB Solid state FLASH memory
- Hardware Watchdog

Network Interface:

- 10/100 Base-T Ethernet (RJ45)

Device Interface:

- 1 Serial port (RS-232, 19200 8N1)

Mechanics:

- Aluminum frame
- Attachment rail for optional and custom mounting tools

SOFTWARE

Operating System:

- Multitasking embedded µCLinux

Supported Protocols:

- PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP, FTP, TFTP, HTTP

Application Services:

- HTTP server, CGI
- FTP client
- Telnet server
- SSH server and client
- Temperature sensor
- Real Time Clock
- Syslog
- DHCP server and client
- Status querying using SMS

Management and Configuration:

- Web user interface
- Console port
- Telnet

2 Physical Interfaces

The Arctic unit contains three panels for interface connections and status indication. These panels are:

1. **Front panel:**

   The front panel configuration is shown in figure 2. This panel includes all connectors and switches for the device operation, optional input/output connectors and the connectors for network and serial interface.

2. **Back panel:**

   The GPRS antenna connector and SIM card holder are shown in figure 6.

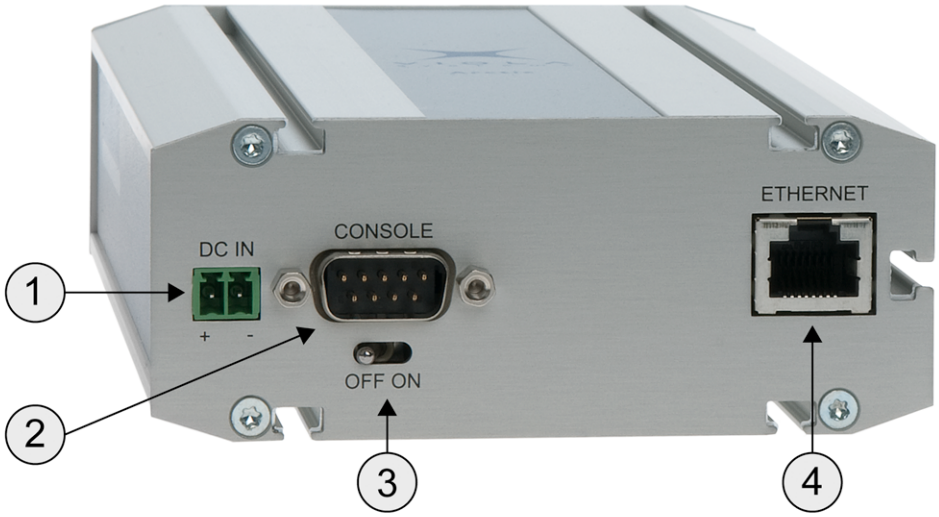
3. **Side panel:**

   The side panel as shown in figure 7 contains all LEDs which indicate the status of the device.

2.1 Front Panel Description

The front panel of the Arctic GPRS Router consists of the following connectors and switches:

Figure 2. *Front panel description*



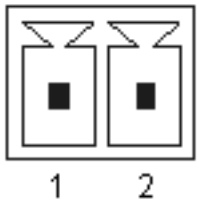
1. Power supply connector
2. Console serial port (RS1)
3. Power switch
4. Ethernet

The Arctic has rails to enable wall or rack mounting. The front panel contains slots for nuts or other mounting accessories (optional) in order to gain access to these rails.

Power Supply Connector

The Arctic has a 10 – 26 VDC power supply connector as shown in Figure 3.

Figure 3. *Power supply connector*



- Pin 1 is positive (+)
- Pin 2 is negative (–)

The unit is protected against reversed polarity.

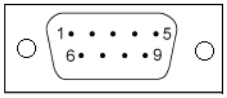
Power Switch

Enables or disables the operation of the Arctic.

Serial Port (RS-232 console)

Arctic has one serial port connector. This is 9-pin male connectors (DB9). A null modem cable may be used to connect the Arctic to a PC (19200 8N1, no handshaking). The Arctic's DB9 (DTE) Male connector is shown in figure 4:

Figure 4. *DB9 male connector*



The serial port 1 is a full RS-232 port. The pin description of this port is as follows:

Table 1: RS-232 Port PIN Description

Pin Number	Name	Direction	Explanation
1	DCD	IN	Data Carrier Detect
2	RXD	IN	Received Data
3	TXD	OUT	Transmitted Data
4	DTR	OUT	Data Terminal Ready. Handshake output
5	GND		Signal ground
6	DSR	IN	Data Set Ready. Handshake input
7	RTS	OUT	Ready To Send. Handshake output
8	CTS	IN	Clear To Send. Handshake input
9	RI	IN	Ring Indicator

Ethernet Connector

Arctic has an RJ45 connector for 10/100 Mbps Ethernet connection. Maximum length of the Ethernet cable is 100m.

Note!
The cross-connected cable is only for connecting the Arctic to the PC's network interface card. When connecting to a local network (e.g. hub or switch), a direct Ethernet cable must be used.

The figure and pin description of the Arctic's RJ45 Ethernet connector is as follows:

Figure 5. *RJ45 Ethernet connector*

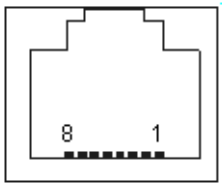


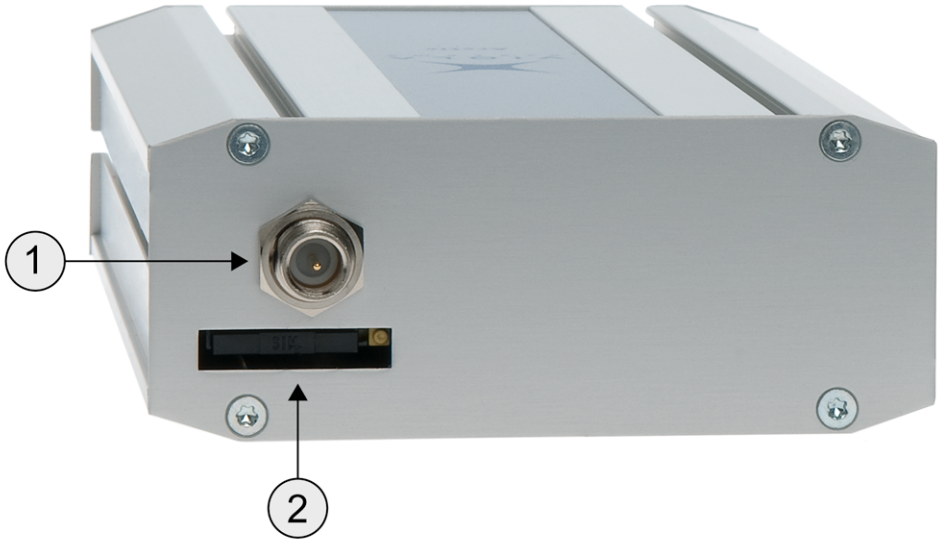
Table 2: RJ45 Ethernet connector PIN Description

Pin Number	Name	Direction	Explanation
1	Rx+	IN	Data Receive Positive
2	Rx–	IN	Data Receive Negative
3	Tx+	OUT	Data Transmit Positive
4	NC	-	-
5	NC	-	-
6	Tx–	OUT	Data Transmit Negative
7	NC	-	-
8	NC	-	-

2.2 Back Panel Description

The Arctic GPRS Router has an antenna connector and a slot for a SIM card on the back panel.

Figure 6. *Back Panel*



1. FME connector for an antenna.
2. SIM Card slot.

Note!

It is recommended NOT to insert or remove the SIM card while the GPRS module is in operation. The SIM card contents may become corrupted if the card is removed while the GPRS module is writing data to it.

2.3 Side Panel Description

The side panel of the device contains ten LEDs which are used to indicate the status of the Arctic and only five of them are connected. The LEDs are numbered from 1 to 10 starting from the rear panel side. A detailed description of each LED is listed below:

Figure 7. *LED Description*

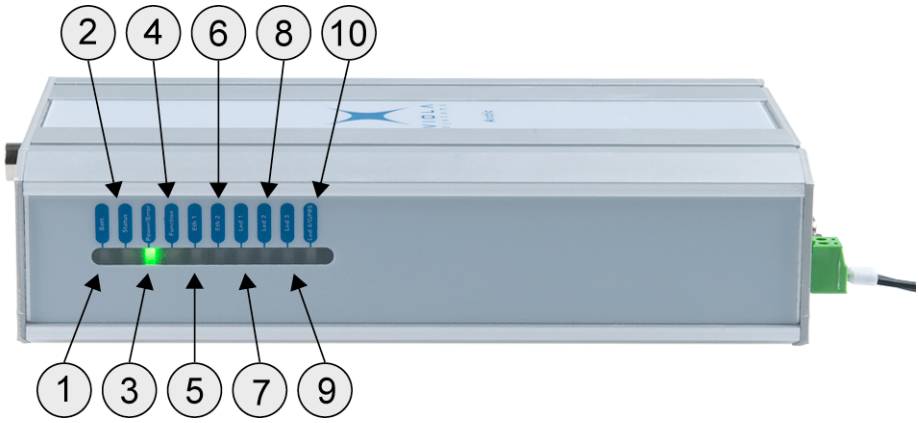


Table 3: LED Description

LED Number	LED	State	Description
1	Battery		Not connected
2	VPN	ON Blinking OFF	VPN connection is up VPN onnection is starting VPN connection is disabled
3	Power/Error	ON OFF	Operating power is turned on Operating power is turned off
4	System Function	ON Blinking	Device is starting Device is operating normally
5	Eth 1	ON Blinking OFF	Ethernet link is up Ethernet link is transferring data Ethernet link is down
6	Eth 2		Not connected
7	LED 1		Not connected
8	LED 2		Not connected
9	LED 3		Not connected
10	LED 4/GPRS	Blinking OFF	GPRS is starting or transferring data GPRS is inactive

2.4 Product Information Label

The product information label on the underside of the Arctic contains the following information:

1. Product type
2. Serial number
3. MAC address

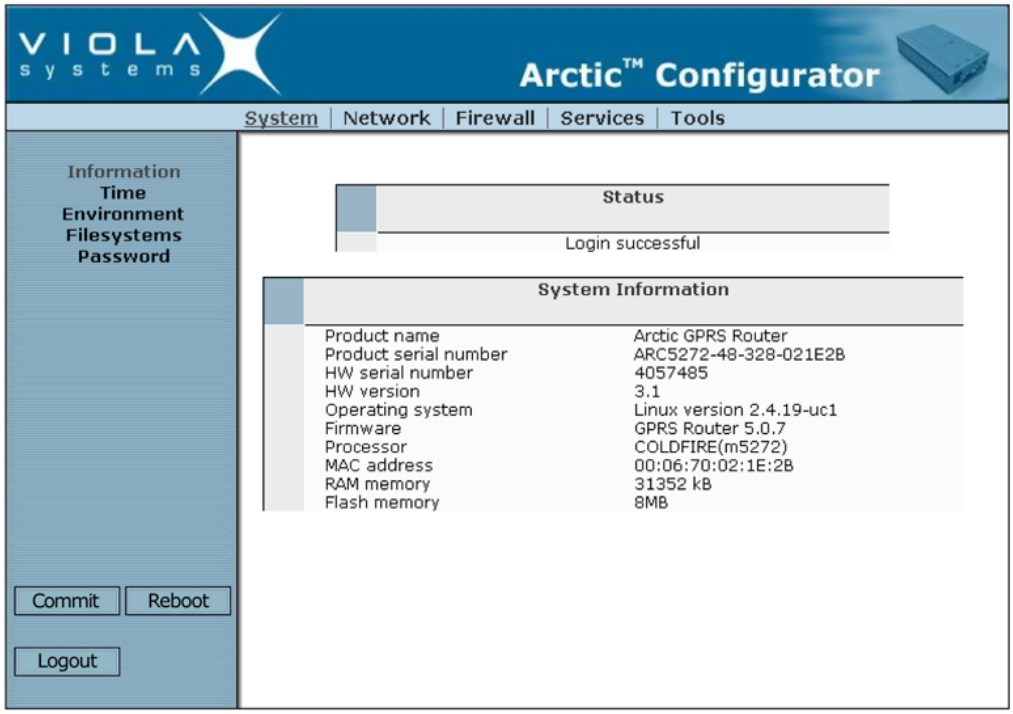
   The Ethernet address (MAC address) of the unit is printed on the product label (Figure 7). Each address code starts with the digits “00:06:70”, but the remaining six digits are unique for each unit.

Figure 8. *Product Information Label*

2.5 Firmware Version

The Arctic firmware version may be checked from the Viola Configurator startup page (System -> Information). It is also possible to get the firmware version by issuing command *firmware* in console.

Figure 9. *Firmware Version*



This manual describes the series 5 firmware version **GPRS Router 5.0.7**.

3 Getting Started

3.1 Unpacking the Arctic

Arctic is delivered in a bulk package containing only the device itself.

A separate Arctic Accessory Kit (ordered separately) contains the following items:

- Power supply and cable
- Cross-over Ethernet Cable
- Null modem cable

If any of the items are missing or damaged, please contact Viola Systems Ltd. All packaging materials are recyclable. Viola Systems urges its customers to follow environmental regulations regarding the disposal of all the materials.

3.2 Installation of the Arctic

The Arctic can be installed horizontally on a flat surface e.g. on a desk or a rack.

When installing Arctic models with wireless connectivity options, it should be remembered that high-frequency radio waves need to be taken into account. The surrounding environment affects the range of radio signals. Therefore, if you are using an Arctic with antennas directly mounted to the antenna connector, try to avoid placing the Arctic where the radio signal might be disturbed (“shadowed”) by nearby obstacles. Also large metallic surfaces (racks) may have a highly detrimental effect on the antenna performance. In case of metal racks or surfaces, it is recommended to use an external antenna with an appropriately selected cable. By following these precautions, the Arctic may be installed more freely.

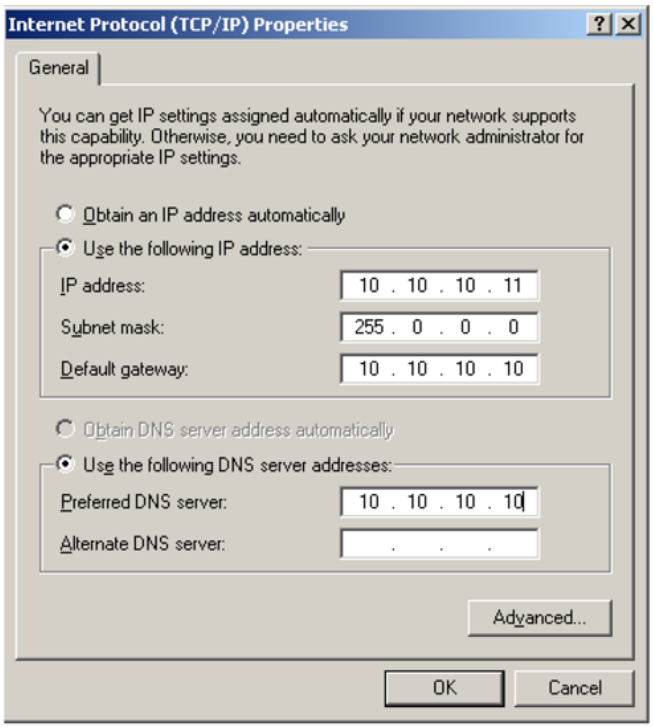
The aluminum case of the Arctic contains rails for wall mounting. Both broad sides contain two rails and the narrow side opposite to the LED panel contains one rail. These rails allow a flexible selection of the optimum mounting direction. To mount the Arctic on a wall using optionally available mounting tools can be used.

3.3 Setting of the IP Address Using an HTML Browser

This is the recommendable way to set up the network parameters. It is an easy-to-apply solution if the computer used for configuration has been properly configured. Follow the procedure listed below:

1. Connect to the Arctic using your HTML browser. The default IP address of the Arctic is “10.10.10.10” (netmask “255.0.0.0”). Computer connected to Viola Arctic device can use for example IP address 10.10.10.11.

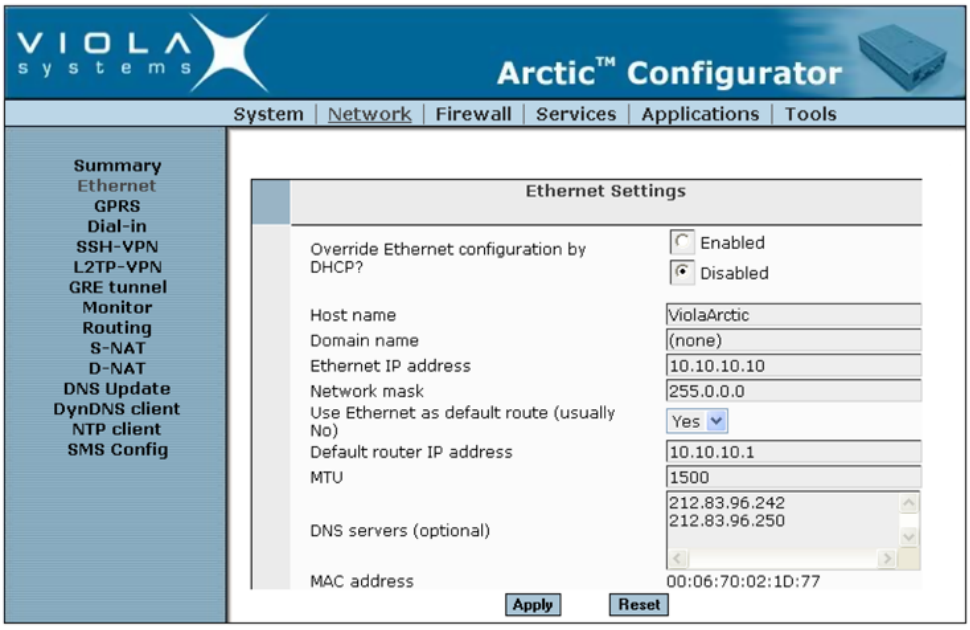
Figure 10. *IP Properties*


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 10 . 11
Subnet mask: 255 . 0 . 0 . 0
Default gateway: 10 . 10 . 10 . 10
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 10 . 10
Alternate DNS server:
Advanced...
OK
Cancel

2. From the initial page, click **Start Configurator** and enter login information in the following page. Username is *root* and by default no password is set (just leave the field empty).

3. Navigate to Network -> Ethernet page.

Figure 11. *Ethernet Settings*



4. Enter the Ethernet IP address (and other network settings) of your choice and click Apply and then Commit (on bottom of page) to store the settings.
5. Reboot the Arctic for the settings to take effect.

Note!
Arctic default password is *empty*. Remember to set the password before connecting the Arctic device to a public network (Chapter 5).

3.4 Setting of the IP Address Using a Console

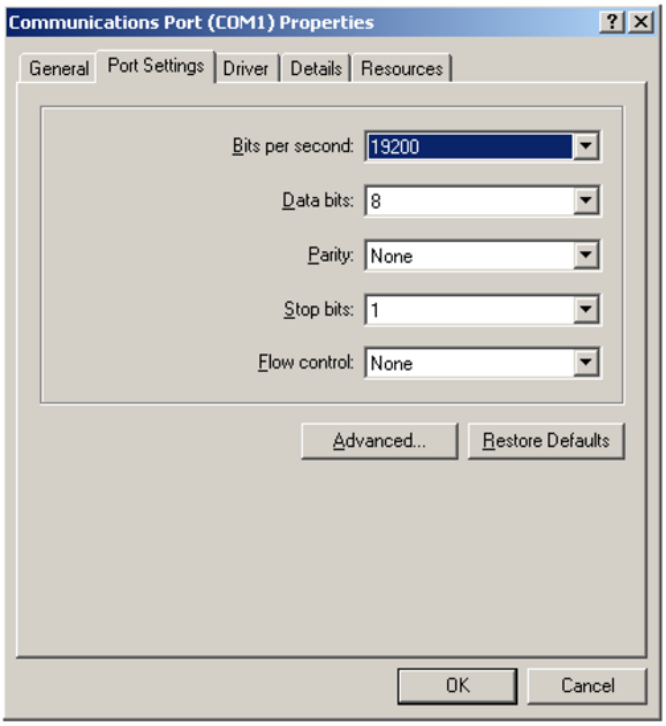
Before installation, you need to find out the required network settings. These include the **IP Address**, **Netmask** and **Gateway Settings** used by the Arctic. The local network administrator can provide them to you or you can ask for them from your Internet Service Provider.

Note!
If possible, it is recommended to use an HTML browser to set up network settings as described in the next chapter. If using a console, please follow the procedure below:

1. Before you start, turn off the power from all devices and check that the power switch of the Arctic is in the “OFF” position.
2. Connect a serial cable (crossover) to the console serial port (RS1) and an Ethernet cable to the RJ45 connector.
3. Switch the Arctic on by toggling the power switch to “ON” position.

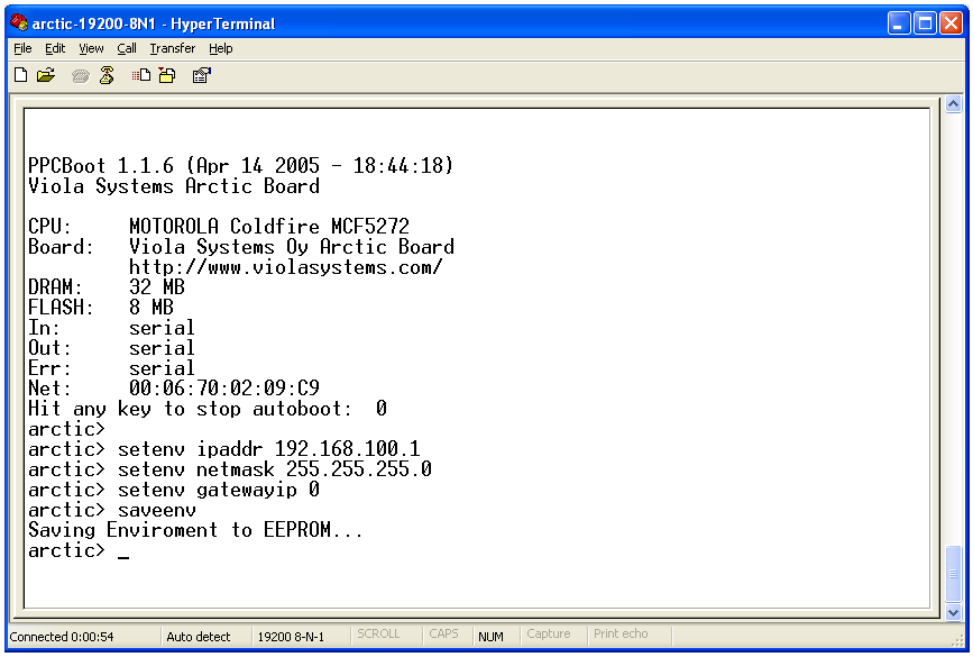
4. Connect to Arctic using COM port and terminal program (Hyperterminal). Serial settings for console (RS1) are 19200-8-N-1 and "Flow control set to none".

Figure 12. *COM1 Properties*



5. Stop the PPCboot to get the “Arctic>” command prompt. Set the IP address and netmask using command “setenv”.

Figure 13. *Arctic COM1 Hyperterminal*



6. Save the setting with command “saveenv”.
7. Reboot the Arctic for the settings to take effect.

Note!
Default gateway value (gatewayip) is usually set to zero (0) because GPRS or VPN is used as default router.

4 Arctic Configurator Tool

The Arctic Configurator is a tool which allows the user to manage the properties of the Arctic device by using a user-friendly, www-based interface. You only need a computer with an HTML browser and a working connection to the Arctic to be able to use the web configurator.

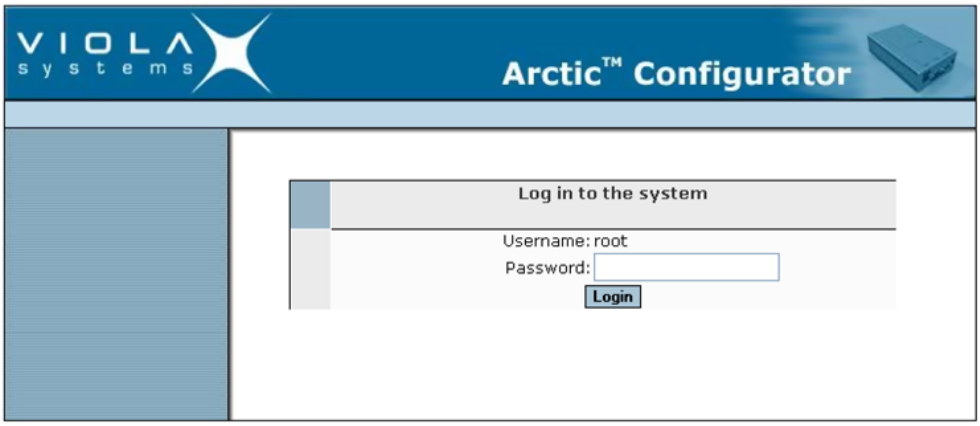
With the Arctic Configurator, you can set important parameters, receive status information, and set variables that control which applications and processes run on the Arctic board.

4.1 Login to Arctic Configurator

To start using the Arctic Configurator, open the URL where the Arctic is located and it has to be configured. On the Viola Arctic main page, select the **Start Configurator** link.

Figure 14. *Start Configurator*

Figure 15. *System Log-in*



Initially, the Arctic Configurator will ask you for the password for the Arctic device root-account. Enter the correct password in the box provided and press the login-button to start the Arctic Configurator.

Note!
Default password for root is empty. Remember to set the password before connecting the device to a public network.Password can be changed from System -> Password menu (Chapter 5).

4.2 General Usage of the Arctic Configurator

After a successful login, the Arctic Configurator will display the main screen. This consists of the main navigation menu on the top, the secondary navigation bar on the left, and the main screen containing the currently active content and controls.

When the program starts for the first time, the System/Information screen will be shown in the main content area. The main navigation-menu on the top of the screen is used to navigate between the different subsets of settings available. Selecting an item from the main menu will display the available items related to this subset in the secondary navigation bar, selecting the first of these to be shown in the main content area.

The secondary navigation-bar on the left contains the groups of parameters in this subset. Selecting an item from this menu will display the content related to the selected group in the main content area. In the bottom of the secondary navigation-bar is a group of three buttons which are always visible: **Commit**, **Reboot** and **Logout**. The Commit-button is used to save the memory-resident data for "soft" parameters permanently to non-volatile memory. Note that the values for the previous parameters are not saved to non-volatile memory unless the Commit-button is pressed. The Reboot-button, as the name suggests, will reboot the Arctic. The Logout button will end the current session and return to the login-screen.

5 Arctic Software Configuration

5.1 System Menu

The System-menu contains items that are relevant to the Arctic board itself. It allows the user to view information about the system or the current executing environment and to set the date and time.

Information – submenu contains general information about the Arctic device. Information on this submenu should be provided if possible when contacting Viola Systems technical support.

Time – submenu contains time information. Arctic has a real time clock with battery backup and time information may be adjusted here.

Note!
Updated time data is not saved permanently until the **Commit** button is pressed. Until then, it will be stored only in RAM memory.

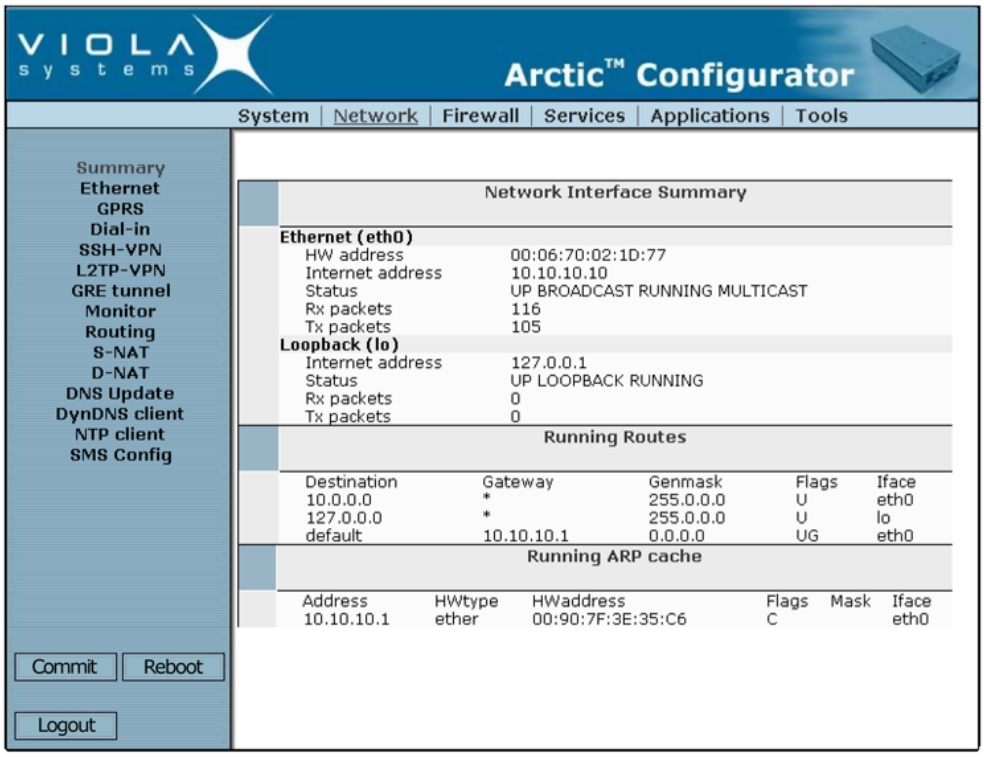
Environment – submenu contains information about the Arctic device memory usage, uptime and inside temperature.

Password – submenu contains password changing. The default password is blank. When changing the password for the first time, the same password has to be written in all three boxes.

5.2 Network Menu

Through the Network-menu you can access sub items to control the various network interface properties. The menu contains items for Ethernet, VPN and GPRS interfaces. Also Email, Proxy and firewall settings are located in this submenu. The **Network Interface Summary page** shows which interfaces are up and also routing information:

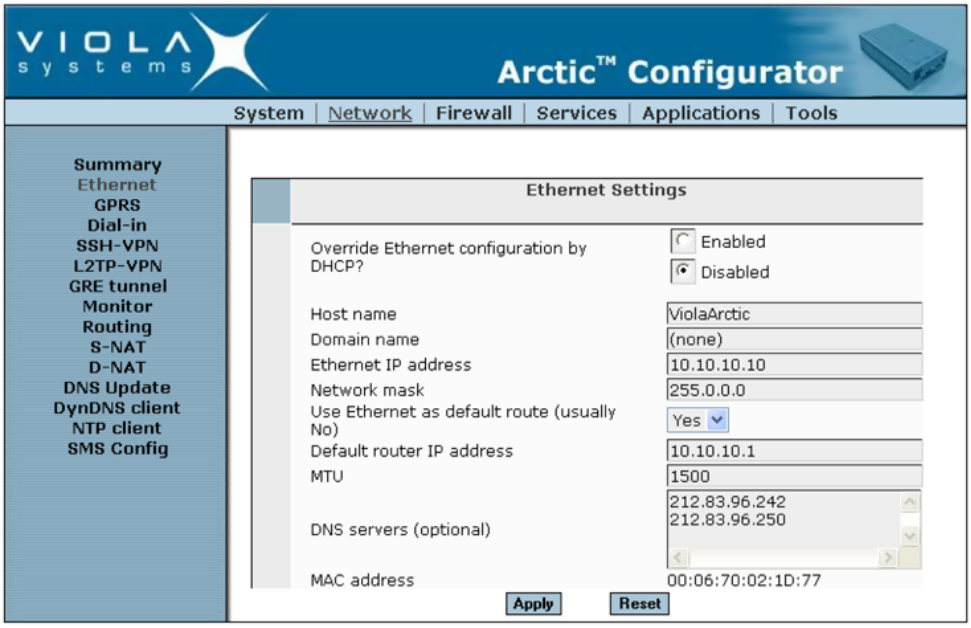
Figure 16. *Network Interface Summary*



5.2.1 Ethernet

Configuration for the Arctic Ethernet Interface:

Figure 17. *Ethernet Settings*



Override Ethernet configuration by DHCP – If this parameter is Enabled, Arctic gets the IP address and other related information from a local DHCP server. When enabled, all other settings are disabled on this page.

Host name – Sets the Arctic device hostname. This is important to set up correctly when using a Viola M2M Gateway and VPN.

Every Arctic connected to Viola M2M Gateway must have unique hostname.

Domain name – Domain name for name resolution (optional).

Ethernet IP address – IP address used by *eth0* interface.

Network mask – Network mask used by *eth0* interface.

Use Ethernet as default route – Set this to “Yes” only when using Ethernet as default gateway/router. This parameter overrides next parameter “Default Route IP Address”, so as long this parameter is set to no, next parameter has no affect. Usually this is set to “No”, because either GPRS on VPN is used as default route.

Default Router IP address – Default router (or default gateway) used when the direct route to host or network is not known. This parameter applies to eth0 interface only. When GPRS or VPN is used as default gateway this parameter has to be set to 0.

MTU – MTU for Ethernet interface (usually 1500).

DNS servers (optional) – Name server IP (DSN) address for resolving host names to IP address and vice versa.

Applicable when GPRS parameter “DNS servers” is set to “User defined”.

Table 4: Ethernet LAN Specificatons

Speed	10Base-T, 100Base-TX
Duplex	Half and Full
Auto-negotiation	Yes
Recommended cabling	Cat5 or better

5.2.2 GPRS

GPRS settings include APN and other settings for GPRS network connectivity. More details of GPRS connectivity is in Chapter *GPRS*.

GPRS enabled – When set to yes, GPRS interface is automatically attached to GPRS network.

Access Point Name (GPRS) – GPRS Access Point (APN) name where the connection is made.

PIN code – SIM card pin code.

DNS servers – When set to “User defined”, DNS servers from Ethernet page are used. If the parameter is set to “From GPRS network” Arctic receives DNS server IPs automatically from GPRS network.

Led indication – In Data only mode, GPRS LED blinks green when transmitting data. In Informative mode, LED blinks also when connected to GPRS network without data transfer (GPRS context is active).

GPRS username – Username used for authentication if APN requires it.

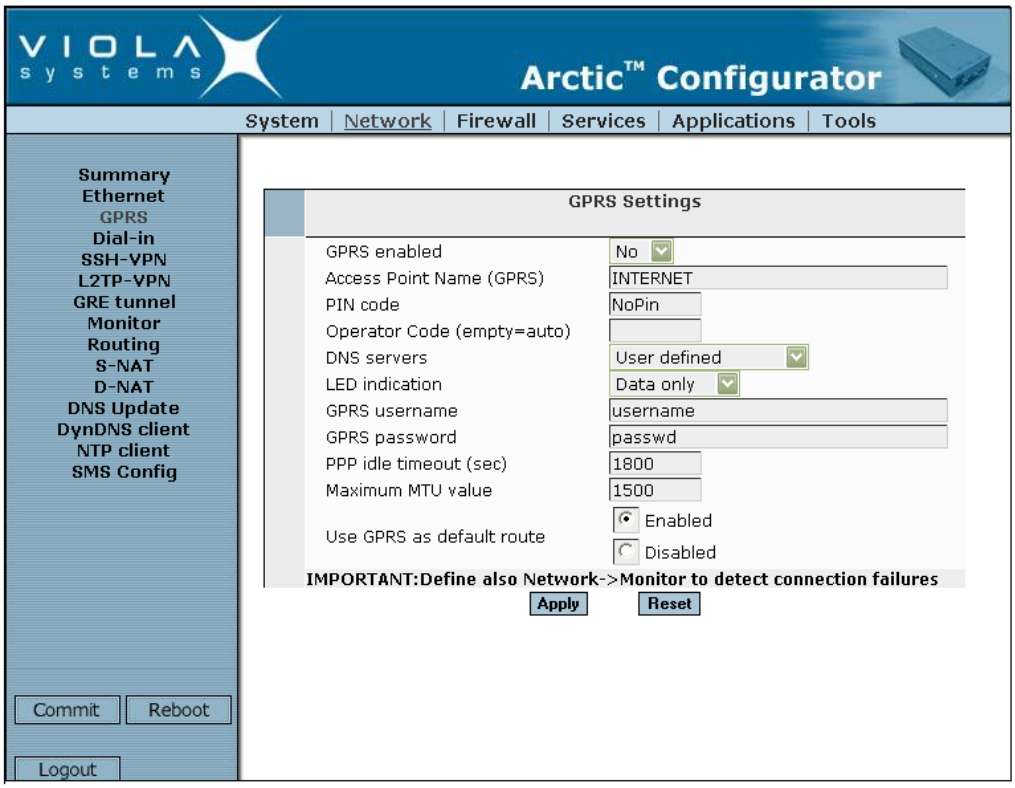
GPRS password – Password used for authentication if APN requires it.

PPP idle timeout – Maximum idle time for GPRS interface. If the GPRS interface has been idle (no traffic) for this period, the GPRS connection is restarted.

Maximum MTU value – MTU (Maximum transfer unit) for GPRS.

Use GPRS as default route – If enabled, GPRS is used as default route. Ethernet default gateway has to disabled (Parameter “Use Ethernet as default route” set to “No” in Network -> Ethernet).

Figure 18. *GPRS Settings*



5.2.3 Dial-in

Configuration for the Arctic PPP dial-in Interface.

Dial-in enabled – When enabled, PPP connections can be made to Arctic (GSM data).

Require authentication (PAP) – When set to *yes* password authentication is used for incoming data calls.

Required username – PAP username allowed login.

Required password – PAP password used for authentication.

Idle timeout – Idle time before PPP connection is terminated.

Local IP address – IP address used in PPP peer.

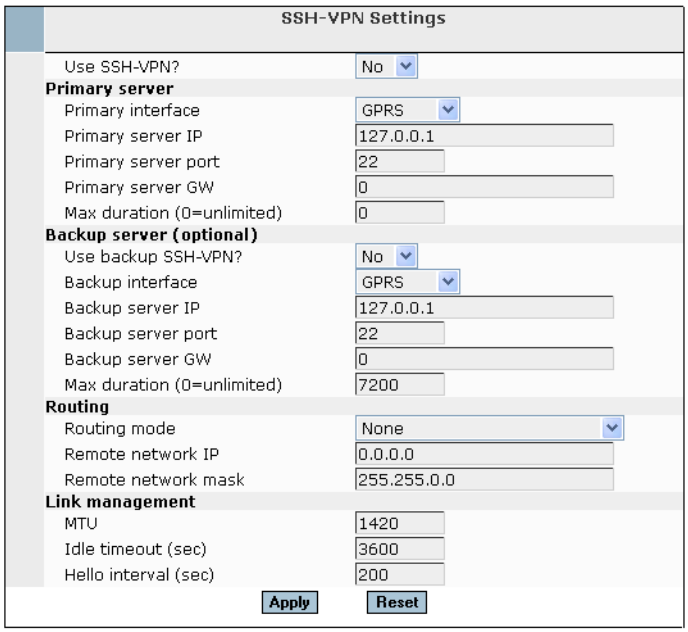
Peer's IP address – IP address used in PPP peer.

Maximum MTU value – MTU (Maximum transfer unit) for Dial-in connections.

5.2.4 SSH-VPN

Arctic has a VPN client that can be used with the Viola M2M Gateway. For VPN configuration, please refer to the Viola M2M Gateway User's Manual.

Figure 19. *SSH-VPN Settings*



Primary server

Use SSH-VPN? – When set to "Yes" Arctic automatically establishes SSH-VPN connection to primary Viola M2M Gateway.

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway SSH-VPN server.

Primary server port – SSH-VPN TCP port on primary server (default 22).

Primary server GW – If other gateway than default route is needed to reach the Viola M2M Gateway.

Max duration (0=unlimited) – Maximum duration of the VPN connection. On primary server, should be set to zero. With backup server, after this timeout, the primary server is tried again.

Connection start timeout (sec) – Time to wait for the connection establishment.

Connection retry interval (sec) – How often retry the connection.

Connection retry mode – incremental increases the retry inteval on each connection attempt. Constant delay uses the same delay always.

Hello interval (sec) – Hello packet interval for the VPN. This can be used as a keepalive message on very critical links.

Hello failure limit – How many hello-packets can be lost before restarting the connection.

Backup server (optional)

Use backup SSH-VPN? – When set to "Yes", Arctic will try to establish VPN connection to backup Viola M2M Gateway, if the primary cannot be reached.

Primary failure limit – How many times primary must not be reached, before changing to secondary.

Other parameters are same as in primary server. The duration of the connection can be set for example to 3600 seconds, so after one hour connection time to backup server the secondary is tried to be reached.

Routing

Routing mode – Routing mode has three modes:

1. "Tunnel the following network" - This adds the “Remote network IP” to be reached via the SSH-VPN. Parameters “Remote network IP” and “Remote network mask” must be set.
2. "Default route" -> VPN interface is used as default route.
3. “None” -> No routing is added when the VPN is established. The VPN peer IPs can be used for communications.

Remote network IP – Remote network IP behind the VPN (on Viola M2M Gateway side) what is needed to reached by Arctic.

Remote network mask – Netmask for remote network IP.

Link management

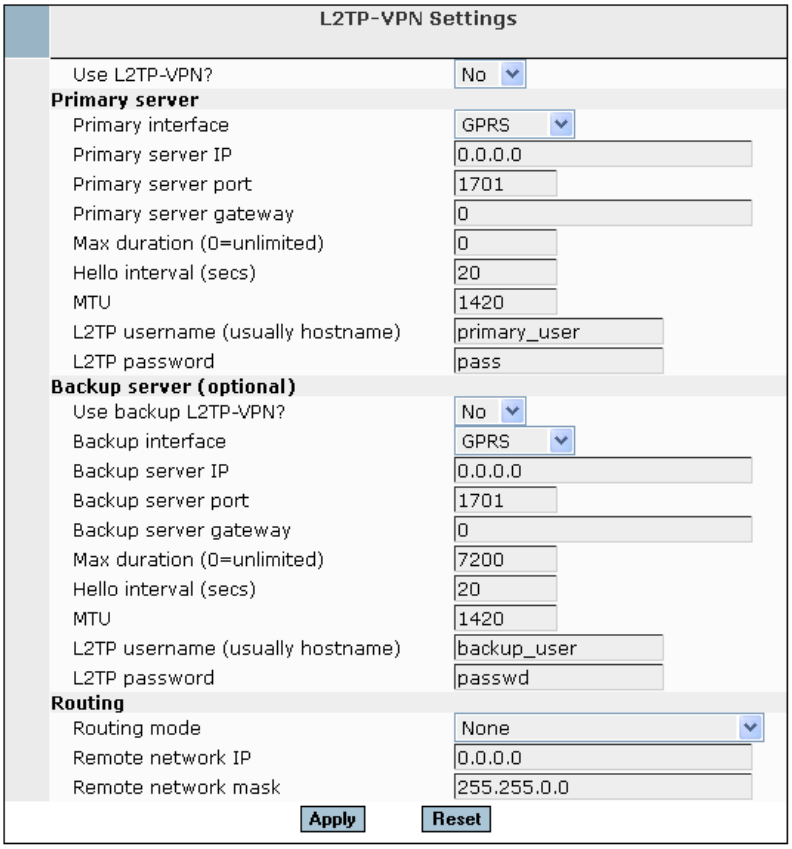
MTU – MTU for SSH-VPN interface.

Idle timeout (sec) – Idle timeout for SSH-VPN interface. If idle timeout is reached, the VPN connection is restarted.

5.2.5 L2TP-VPN

Arctic has a L2TP client that can be used with L2TP server.

Figure 20. *L2TP-VPN Settings*



Use L2TP-VPN? – When set to "Yes", Arctic established L2TP VPN connection with primary Viola M2M Gateway.

Primary server

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway L2TP server.

Primary server port – L2TP VPN server port (UDP, default 1701).

Primary server gateway – If other gateway than default route is needed to reach the Viola M2M Gateway

Max duration (0=unlimited) – Maximum duration of the VPN connection. On primary server, should be set to zero.

Hello interval (secs) – Hello interval for connection keepalive (default 20 seconds).

MTU – MTU for L2TP interface

L2TP username – (usually hostname) - Username for authentication.

L2TP password – L2TP password for authentication.

Backup server

If the primary server cannot be reached, the L2TP VPN connection is established with backup server.

Routing mode

It is used if routing is needed with L2TP interface. Configuration parameters are same as in SSH-VPN.

5.2.6 GRE

GRE tunnel enabled – When set to "Yes", Arctic establish automatically GRE connection

Interface – Interface used to reach the GRE server

GRE server IP – IP address of GRE server

Gw to GRE server* – (ethernet mode) If other gateway than default route is needed to reach the GRE server.

Local GRE interface IP – (usually eth0 IP) - Local IP used in GRE tunnel

Remote GRE interface IP* –Remote IP used in GRE tunnel

TTL value – Time-to-live value for the interface

Checksum* – checksum value.

Incoming key* – authentication key.

Outgoing key* – Outgoing key for the server

Routing

Routing mode – same as in SSH-VPN and L2TP

Remote network* – same as in SSH-VPN and L2TP

Remote network mask* – same as in SSH-VPN and L2TP

*These are optional, please refer to your GRE server documentation

5.2.7 Monitor

Monitor is used for GPRS and VPN connection checking. If connection to the selected IP address is lost, the connection is restarted. Monitor uses ICMP echo (ping) packets to check the connection. The monitor also keeps the connection alive, so that idle timeout do not drop the connections.

ICMP Echo sending – Selects if the monitor is enabled.

This should be always enabled to correct IP.

Interval (sec) – Determines how often the connection is checked by sending ICMP echo packets. The interval should be smaller than GPRS idle timeout (typically max. 2/3 of GPRS idle timeout) in order to have uninterrupted communication.

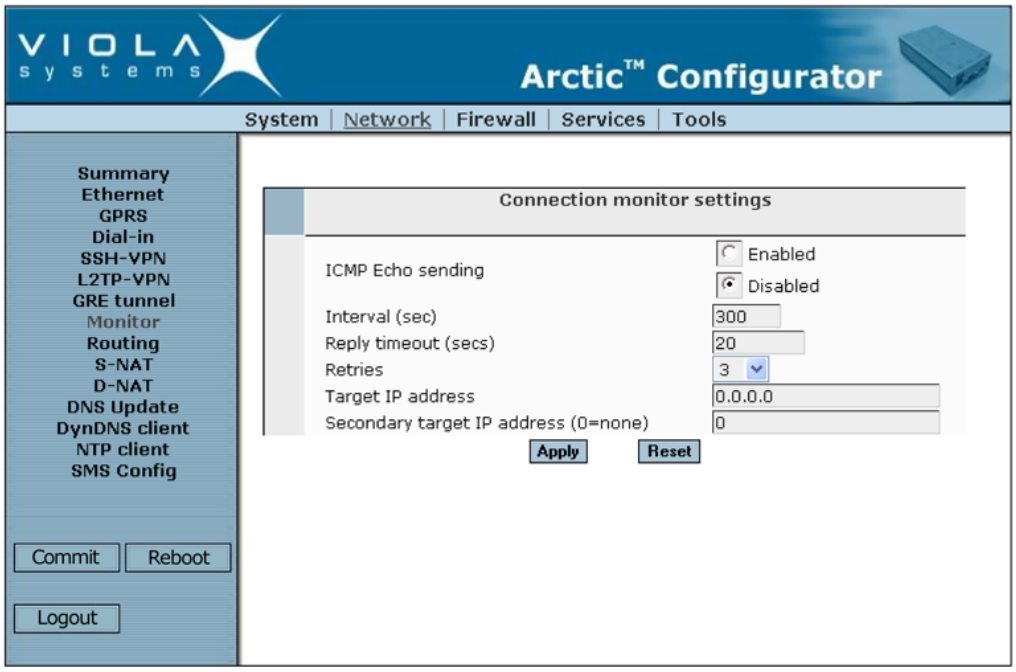
Reply timeout (secs) – The waiting time for reply packets.

Retries – The number of tries before connections are restarted.

Target IP address – The host IP address to which echo packets are sent to.

Secondary target IP address – The secondary host IP address to which ICMP echo packets are to be sent if the sending to primary target host IP address fails.

Figure 21. *Monitor Settings*



Note!

Monitor must be always enabled. When VPN is used, remote VPN peer IP (or other IP reached only via VPN) must be used for connection checking

5.2.8 Routing

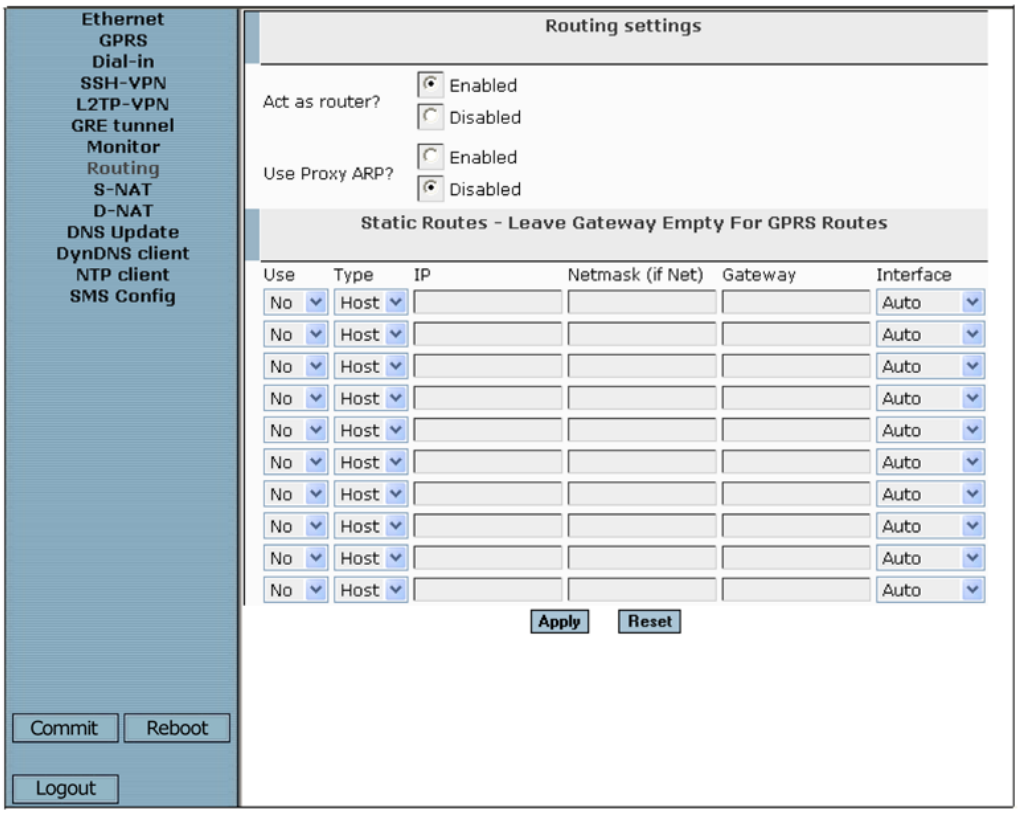
These parameters are used to configure routing settings

Act as router – Enables IP forwarding between interfaces.

Use Proxy ARP – Enables proxy ARP. It can be used with Viola M2M Gateway VPN.

Static routes can be added, if some hosts or networks require static routing settings.

Figure 22. *Routing Settings*



5.2.9 S-NAT

These parameters are used to configure S-NAT (source network address translation) settings. When enabled, private IP address used in local LAN is changed to GPRS interface IP address.

From IP – Only S-NAT connections from the defined IP address are accepted. If defined with wildcard (0/0), all IP addresses are handled the same way (only S-NAT connections are allowed).

5.2.10 D-NAT

These parameters are used to configure D-NAT (destination network address translation) settings. When enabled, packets coming to define GPRS interface port are forwarded to local IP address.

Source IP – D-NAT only connections coming from IP. Wildcard 0/0 means all IP addresses are D-NATted.

Protocol – Chooses which protocol is port forwarded. If “ANY” is chosen, other parametes are disregarded.

Dest.port – Chooses which GPRS interface is port forwarded to local Ethernet.

Redirect to IP – Chooses where port forwarding is done to.

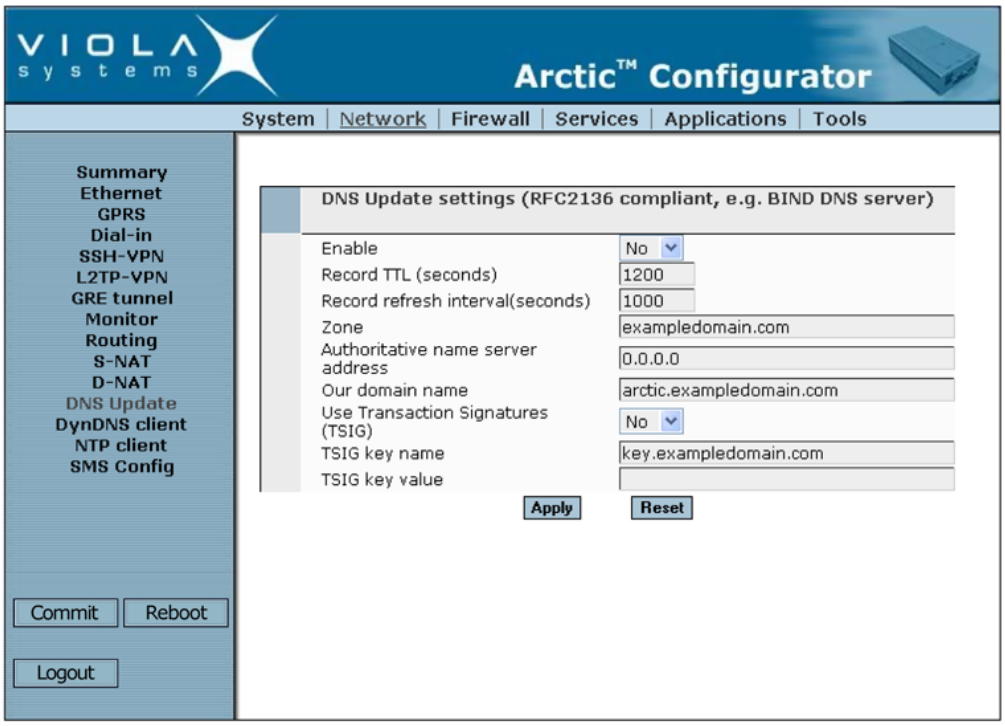
Redir. port – Chooses which port forwarding goes to.

5.2.11 DNS Update

These parameters are used to configure dynamic DNS. Arctic can report its dynamic IP address to a DNS server.

The DNS Update settings are RFC2136 compliant, for example BIND DNS server.

Figure 23. *DNS Update settings*



The server pointed by parameter “Authoritative names server” (eg. company’s own DNS server, for example ISC BIND) must be configured to accept incoming DNS update messages. TSIG keys can be used for better security in DNS updates.

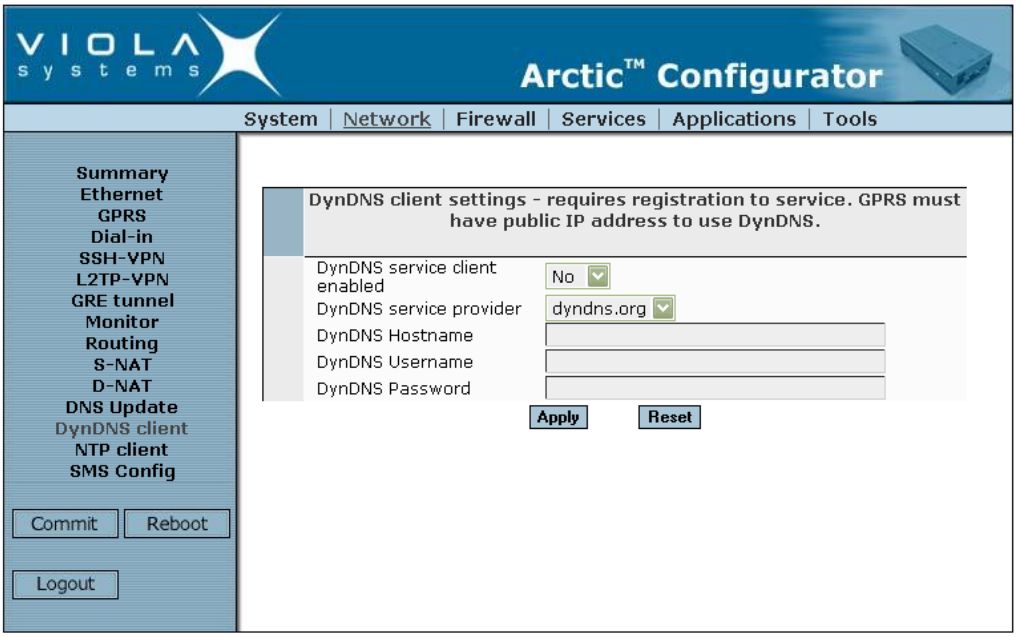
5.2.12 DynDNS Client

This feature can be used with DynDNS service available at http://www.dyndns.org.

Note!

The public IP is required for GPRS and user account from the DynDNS service operator.

Figure 24. *DynDNS Client Settings*



DynDNS service client enabled – Disables or enables dynDNS DNS name update.

DynDNS service provider – Only dyndsn.org currently supported.

DynDNS Hostname – Service provider account hostname.

DynDNS Username – Service provider username.

DynDNS Password – service provider password.

5.2.13 NTP Client

This feature may be used to update the real time clock of Artic using NTP protocol.

NTP server – When set to "Yes", Arctic updates system clock from NTP server.

Query interval – How ofter NTP query is sent.

Minimum time difference (seconds) – Minimal time difference, when the clock is updated.

Maximum time difference – Maximum time difference between local system time and NTP time, when the clock is updated.

Time adjust mode –Adds or subsracts time from the received NTP value.

Time adjust value (minutes) – value to add or substract from NTP value.

5.2.14 SMS Config

This feature may be used to monitor the Artic status and to issue simple commands remotely via SMS messages. For detailed information, refer to “SMS Config Application Note”.

Enabled – Selects whether the SMS Config function is enabled or disabled.

Get commands

Access – Are get commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for get commands.

Require password – Require system password for get commands.

Set commands

Access – Are set commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for set commands.

Require password – Require system password for set commands.

Allow execute commands – Allow execute commands to be run on Arctic.

Other

Reply error to unknown commands – If set to "No", incorrect commands are silently disregarded. If set to "Yes", Arctic will send error SMS.

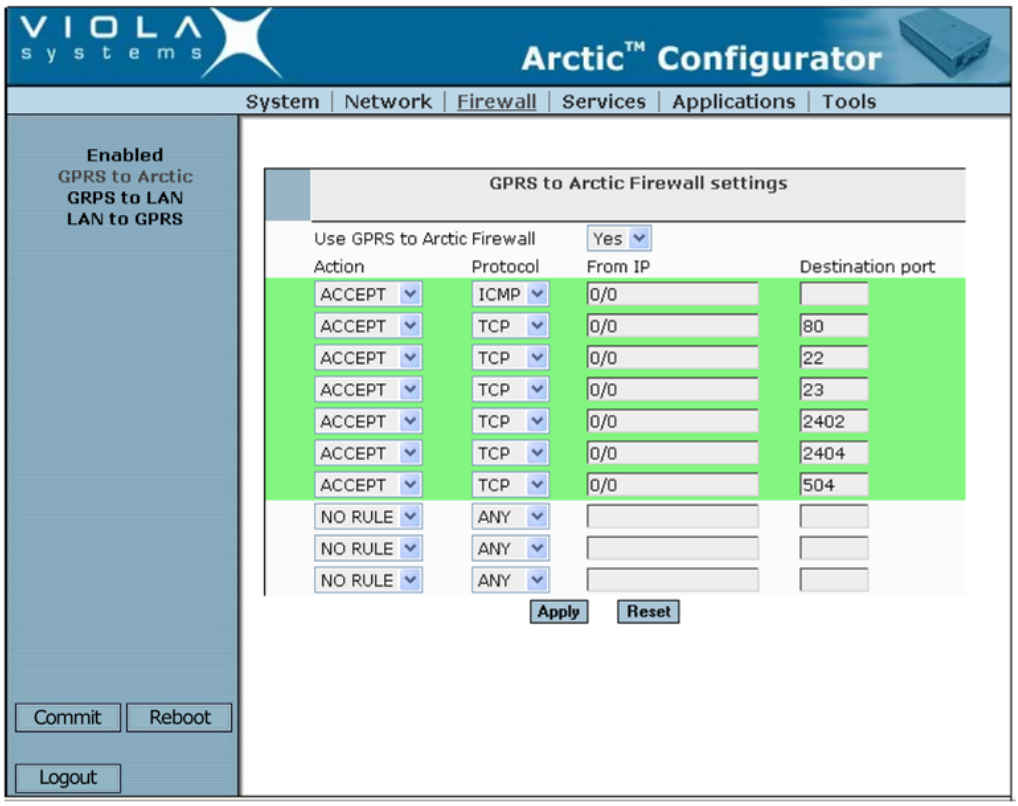
Reply error to unauthorized commands – If set to "No", unauthorized command are also silently disregarded. If set to "Yes", Arctic will send error SMS.

Factory reset command (8 chars min) – Command to issue device back to factory settings. This does not require system password. After issuing this SMS command, Arctic will have factory settings (eg. password is set back to factory default also).

5.3 Firewall Menu

Through the Firewall menu, you can configure built-in firewall of the Arctic. Firewall can be disabled or enabled and separate rules may be created for GPRS to Arctic, GRPS to LAN and LAN to GPRS.

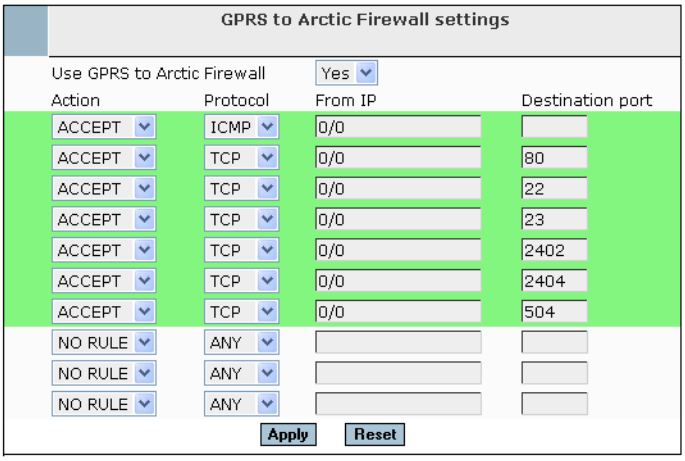
Figure 25. *GPRS to Arctic Firewall Settings*



The firewall rules are processed from top to bottom. If strict rules are wanted, last rule should be DROP.

The parameter “From IP” can be used for limiting access based on IP address. For example “192.168.100.0/24” would limit access only packets coming from 192.168.100.0 network.

Figure 26. *GPRS Settings*



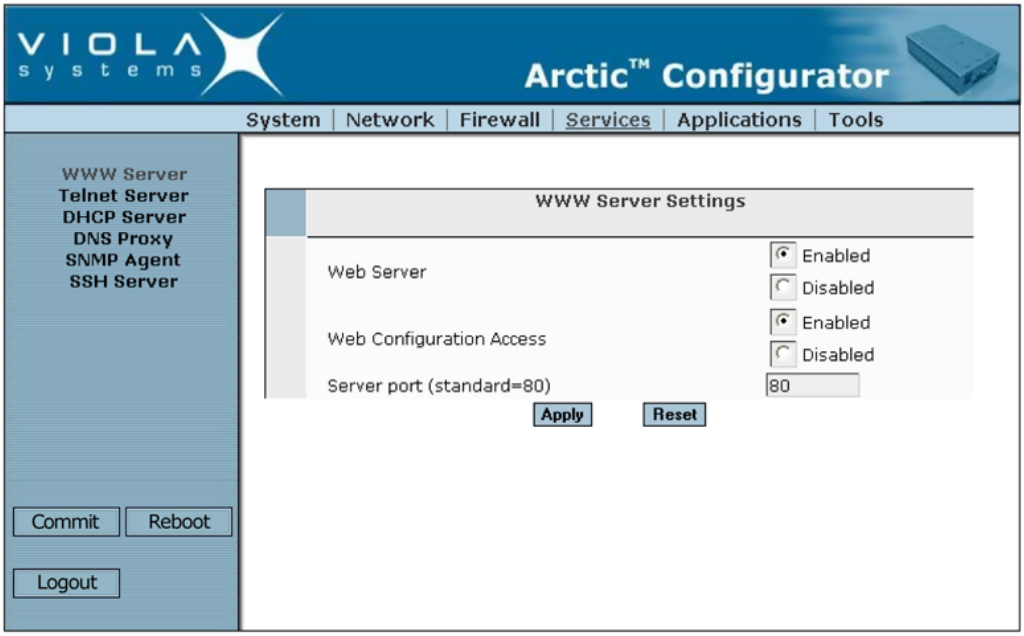
These rules would allow incoming connection to GPRS interface: ICMP, web (TCP port 80) and telnet (TCP port 22) from any IP access.

5.4 Service Menu

5.4.1 WWW

These settings enable or disable the web server functionality.

Figure 27. *Service Menu*



Web Server – Disables or enables the www server.

Web Configuration Access – Disables or enables web configuration access.

Note!
If you disable the web access settings, web configurator stops functioning and you will have to enable it via console if you should need to use it again later.

5.4.2 Telnet

Telnet server may be used to make terminal connections to the Arctic device shell. A more secure way of performing remote management is based on the SSH.

Telnet server – Enables or disables the telnet server.

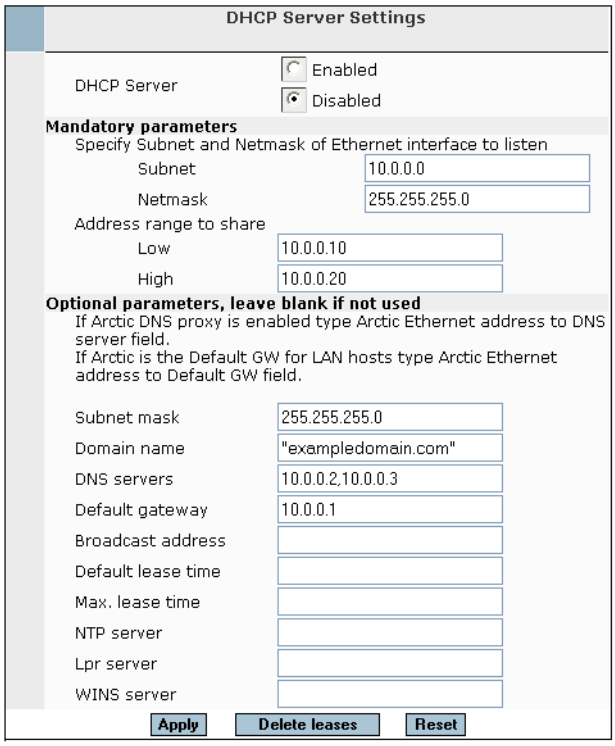
5.4.3 DHCP Server

DHCP server listens to broadcast DHCP queries and assigns IP address for host from the configured pool. If needed, Arctic can act as a DHCP server. This is suitable for small remote networks that have for example few laptops connected to the Arctic via an Ethernet hub or a switch.

DHCP Server

Enables or disables the DHCP server.

Figure 28. *DHCP Server Settings*



Note!
Configuring the DHCP server in an erroneous way may cause your network to function badly or may prevent functioning altogether. Consult your network administrator for necessary information **before** setting up the service.

DNS Proxy

With DNS proxy, computers connected to Arctic Ethernet interface can use Arctic as DNS server. Arctic will forward DNS queries to correct DSN server and local computers DNS setting are not needed to be changed. This can be used with GPRS settings (Network ->GPRS) parameter “DNS servers: From GPRS network”.

DNS Proxy/Forwarder –When set to ”Enabled” Arctic can be used as DNS server for local computers.

SNMP Agent

Arctic supports MIB-II SNMP Agent.

SNMP agent (SNMP Set/Get) – Set SNMP agent enabled or disabled.

Read only SNMP community – read only community string.

Read and write SNMP community – rw snmp community

Server port (standard=161) – Agent listen port (UDP)

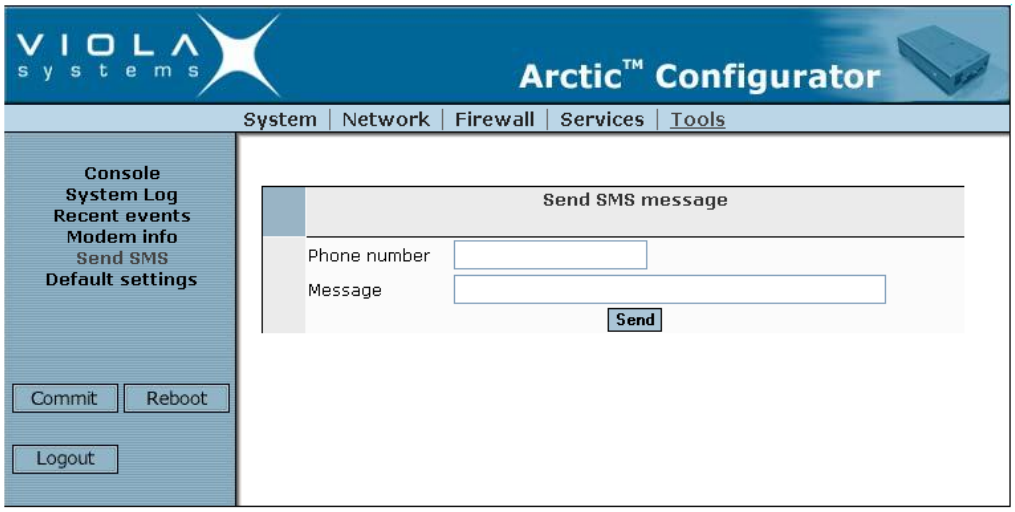
Bind to interface – The interface is used as source address.

5.5 Tools Menu

The Tools menu provides the access to web based tools used for troubleshooting with the Arctic. It is possible to execute simple shell

commands through the Web console. Also GPRS information can be obtained from “Modem Info” menu.

Figure 29. *Tools Menu*



Console

Console can be used for running command over the web interface. Example commands:

```
ping –c 10 172.30.30.1
firmware
```

System Log and Recent events

Arctic system log can be seen on system log and recent event. When support for device is need, full copy&paste from system log is needed.

Modem info

Arctic modem info show information about GPRS and GSM status. Also the signal strength is shown here. This can be used for GPRS connection problems on site.

Send SMS

Arctic may be used for sending test SMS. This can be used for example checking the phone number of current SIM-card.

Default Settings

Arctic may be set to factory default settings from the Tools menu. This restores factory settings excluding network settings.

6 GPRS

The Arctic with GPRS includes a FME connector (male type) for an external antenna. It is possible to use any kind of external 50Ω dual-band antenna intended for GSM frequency bands (quad-band).

In this Chapter, the specialities related to GPRS operation are described.

6.1 Placing Arctic

When choosing the installation site of Arctic models with the GPRS option, please remember that it uses radio waves for data transmission. The surrounding environment affects the behavior of the radio signals. Therefore, if you are using an Arctic with the antenna mounted directly to the antenna connector (without an extension cable), try to avoid placing the unit in a location where the radio signal might be shadowed by nearby obstacles. Note also that large metallic surfaces (racks) or walls with metallic structures (cabling, concrete iron) may highly degrade the antenna performance. In case of metal racks or surfaces, it is recommended to use an external antenna with an appropriate cable. This allows placing of the Arctic more freely.

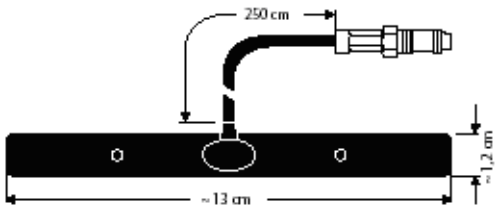
6.2 GPRS Antenna

The Arctic with GPRS includes a FME connector (male type) for an external antenna. It is possible to use any kind of external 50Ω dual-band antenna intended for GSM900 (880–960 MHz) and GSM1800 (also known PCN) (1710–1880 MHz) frequency bands. Connect the antenna directly to the connector provided for the antenna on the back panel of the Arctic unit.

Typically, commercially available antennas are provided with a flexible 50Ω cable having a length of 2–3 meters and having a female type FME-connector.

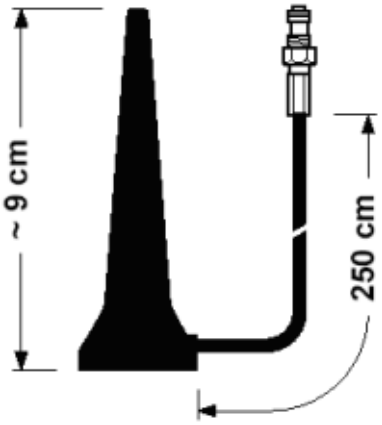
The Arctic GPRS Router is tested with antennas from Hirschmann Rheinmetall Elektronik GmbH. Examples of tested external antennas include the sticker-type and magnetic mount antennas shown in Figure 30 and 31 respectively:

Figure 30. *External Antennas*



MCA 18 90 STRIPE, sticker type patch antenna (above), and MCA 18 90 MH , magnetic mount antenna (right). Both antennas have a FME (female) connector and L=250 cm RG174 cable.

Figure 31. *Magnetic Mount Antenna*



6.3 SIM Card and Card Holder

Standard 3 V SIM cards may be used with the Arctic GPRS Router. A SIM card holder is located on the back panel near the GPRS antenna connector. If you have the PIN code query enabled, check that the Arctic Configurator has a correct PIN code entered in the GPRS submenu. To operate with SIM card follow the procedure below:

1. Power off the Arctic.
2. The SIM card holder contains a tray with a yellow eject button. Push this button in order to eject the tray from the holder.
3. Put the SIM card onto the tray.
4. Insert the tray carefully back to the holder and press the tray until it is locked.

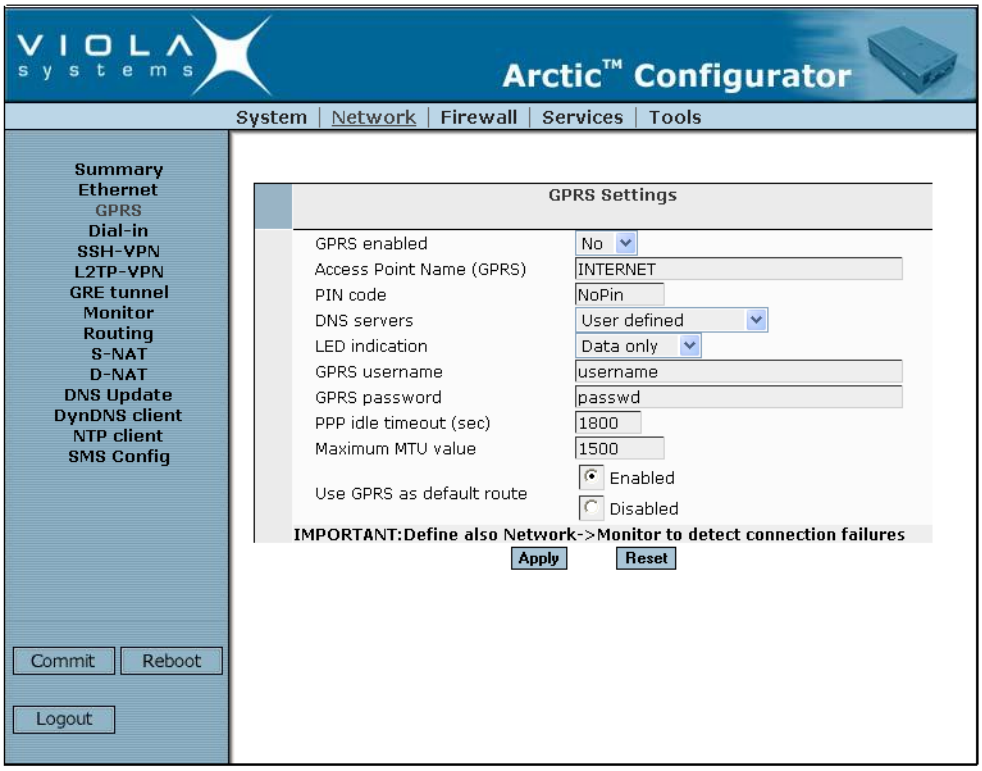
Note!
The card should only be inserted or removed while the GSM module has been placed in shutdown mode. The SIM card holder has a card detection circuit that will in theory allow hot insertion and removal of the card. However, hot insertion and removal are not recommended, since the SIM card content may be corrupted if the card is removed while the GSM module is writing data to it.

6.4 Configuring Arctic's GPRS Settings

1. If your SIM card has the PIN code querying set, make sure you configure the PIN code before inserting the card in the card holder. If PIN querying is not set, you may proceed with the card installation procedure.
2. Connect to the Arctic and log in to Configurator.
3. Navigate to Network page from main navigation bar and select the GPRS sub page. (Network -> GPRS).
4. Set the access point name appropriately (usually “INTERNET”) or “operatorname.com”).
5. Set the GPRS network username and password appropriately if your GPRS service requires authentication.
6. Set default route to *enabled*. With this setup, you are able for example to browse the web.

7. Optionally, set the PIN code and PPP idle timeout.
   - If your SIM card has the PIN code set, type the code into the PIN code field.
   - PPP idle timeout defines the time in seconds how often the Arctic resets the GPRS connection if the connection is idle.
   - ICMP Echo is used to monitor GPRS connection between Arctic and a remote host. If the designated host cannot be reached the GPRS connection is reset. This feature should be always enabled from Network -> Monitor menu.
8. Finally click on **Apply**, wait for the confirmation and then click on **commit** to store the settings. Again, wait for **commit** confirmation.

Figure 32. *GPRS Settings*



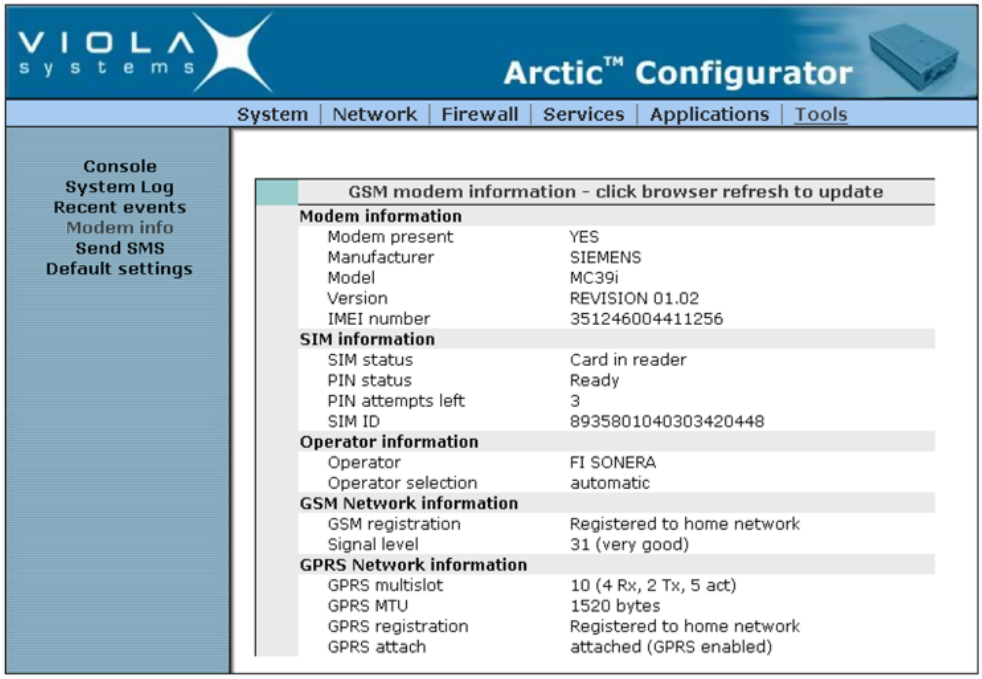
Reboot the Arctic for the settings to take effect. Check GPRS status from Network/Summary Menu.

Note!
It is important to set the correct PIN code with the Arctic Configurator before plugging the SIM card in. If an incorrect PIN is set and the PIN is required by the SIM card, the Arctic will not retry with the wrong PIN, thus avoiding the SIM card lock-up. In such a case, you will need to insert the SIM card to a mobile phone and enter the correct PIN before continuing.

6.5 Useful GSM/GPRS Information

Useful GSM/GPRS information can be obtained from Tool -> Modem Info Menu.

Figure 33. *Useful GSM/GPRS Information*



7 Troubleshooting

This Chapter provides a list of the common problems encountered while installing, configuring or administering the Arctic. If you are unable to resolve your problem, refer to the Warranty and Technical Support Sections at the end of this User's Guide for information about contacting Viola Systems Technical Support representatives.

Q: When setting up routing mode \tunnel the following network", routing to M2M Gateway eth1 does not work?

A: Check that IP forwarding has been enabled and internal firewall does not block packets.

Q: From Arctic Ethernet connection to M2M Gateway Ethernet is not working?

A: Check that IP forwarding has been enabled on Arctic.

Q: If only one public IP is available, can the M2M Gateway be used?

A: Yes, if firewall connected to public IP can forward incoming SSH connections to the M2M Gateway.

7.1 Common Problems

Problem #1

Q: Console does not receive characters.

A: Disable HW and SW handshaking from you terminal software (e.g. Hyperterm or Minicom).

Problem #2

Q: GPRS interface is up but no traffic flows through it.

A: Default gateway in Ethernet settings submenu has to be set as "0" and also default gateway has to be enabled from Network/GPRS menu when using GPRS interface as the default gateway.

Problem #3

Q: GPRS connection is not established.

A: Check that the SIM card has the correct PIN number settings and that it has not been locked after a wrong number was entered three times successively. PIN status can be checked from Tools/Modem Info menu.

Problem #4

Q: GPRS connection is ended after approximately two minutes.

A: You have enabled connection checking from Network/Monitor menu but not set the correct IP to GPRS "ICMP Echo settings".

Specifications

Technical Specifications	
Processor	32-bit 48 MHz RISC Processor
Memory	▪ 32 MB RAM ▪ 8 MB Flash ROM
Network Interface	▪ 10/100 Base-T. Shielded RJ45 ▪ Ethernet (IEEE 802.3) ▪ 1.5 kV isolation transformer
Serial Device Interface	▪ 1 x Male DB9 connector DTE ▪ 15kV ESD and short circuit protection ▪ RS-232, 19200 bit/s, 8 data bit, 1 stop bit, no parity (console)
Power Requirements	▪ 10 – 26 VDC, less than 500 mA (1–4 W power consumption) ▪ Resettable fuse and ESD protected input ▪ External 110–230 VAC adapter (optional)
Temperature Range	▪ Operating: –20 to 70 ^{o}C ▪ Storage: –30 to 85 ^{o}C
Relative Humidity	Operating: 5 to 85 % RH non-condensing
Operating System	µCLinux embedded multitasking operating system
Network Protocols Supported	PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP,FTP, TFTP, HTTP
Tunneling (VPN)	▪ SSH-VPN client (requires Viola M2M Gateway) ▪ L2TP-VPN client (requires Viola M2M Gateway) ▪ SSH client
Management	WWW, SSH, Telnet and console FTP, TFTP and HTTP software update
Routing and Firewall	Static routing, proxy ARP, port forwarding, IP masquerading/NAT, firewall
Serial Device Connectivity	▪ Device server application (Serial GW) ▪ Simultaneous GPRS, CSD and SMS ▪ SMS configuration and status reporting
Dimensions and Weight	▪ Models in aluminum frame: ▪ Size: 180 mm x 110 mm x 45 mm (WxLxH) ▪ Weight: 0.7 kg ▪ Attachment rail for optional and custom mounting

Limited Warranty

Coverage

Viola Systems warrants this hardware product to be free from defects in materials and workmanship for the warranty period. This non-transferable, limited warranty is only to you, the first end-user purchaser. The warranty begins on the date of purchase and lasts for the period specified below:

Arctic GPRS Router : one (1) year

Excluded Products and Problems

This warranty does not apply to: (a) Viola Systems software products; (b) expendable components such as cables and connectors; or (c) third party products, hardware or software, supplied with the warranted product. Viola Systems makes no warranty of any kind on such products which, if included, are provided "AS IS." Excluded is damage caused by accident, misuse, abuse, unusually heavy use, or external environmental causes.

Remedies

Your sole and exclusive remedy for a covered defect is repair or replacement of the defective product, at Viola Systems' sole option and expense, and Viola Systems may use new or refurbished parts or products to do so. If Viola Systems is unable to repair or replace a defective product, your alternate exclusive remedy shall be a refund of the original purchase price.

The above is Viola Systems' entire obligation to you under this warranty. IN NO EVENT SHALL VIOLA SYSTEMS BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, USE, OR PROFITS EVEN IF VIOLA SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Viola Systems' liability exceed the original purchase price of the device server. Some states or countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

You must notify Viola Systems within the warranty period to receive warranty service. During the warranty period, Viola Systems will repair or replace, at its option, any defective products or parts at no additional charge, provided that the product is returned, shipping prepaid, to Viola Systems. All replaced parts and products become the property of Viola Systems. Before returning any product for repair, customers are required to contact the Viola Systems.

Technical Support

Contacting Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: http://www.violasystems.com

Recording Arctic Information

Before contacting our Technical Support staff, please record (if possible) the following information about your Arctic product:

Product name:

_____

Serial no:

_____

Note the status of your Arctic in the space below before contacting technical support. Include information about error messages, diagnostic test results, and problems with specific applications.

_____

_____

_____